Cybersecurity Takes Center Stage yet Progress is Interrupted, finds 2015 U.S. State of Cybercrime Survey

Despite increase in reported incidents, few have solidified cybersecurity processes; Information sharing comes front and center

NEW YORK and FRAMINGHAM, Mass. July 9, 2015 – PwC US and CSO today released the 2015 U.S. State of Cybercrime Survey. The survey reveals that despite a year of highly public and destructive cyberattacks, few organizations' cybersecurity policies and processes are providing better protection than a year ago. However, this year's findings show government agencies and corporate board of directors are taking an increased role when it comes to cybersecurity practices. More than 500 executives from U.S. businesses, law enforcement services and government agencies share their views in the survey, which was a collaborative effort among PwC, CSO, the U.S. Secret Service, and the Software Engineering Institute CERT® Division at Carnegie Mellon University.

"2015 has been a watershed year for cybercrime. Headlines in 2015 make it clear that the threat is increasing, yet much more must be done to stem losses and damages. High profile incidents teach us over and over again that no system is immune – and that speed to identify and respond is of the essence when it comes to combatting cyber threats and reducing the risk and associated damages," said David Burg, Global and U.S. Cybersecurity leader, PwC. "Keeping pace with today's sophisticated adversaries is not simply a matter of an increase in cybersecurity spending. Results of this year's survey highlight opportunities and potential for information sharing across industries and regions. Greater transparency and visibility into the threat landscape can lead to more action from corporate boards, rapid and informed decision-making, appropriate investments in spend and resources, and greater agility when responding to threats."

This year, 76 percent of respondents said they were more concerned about cyber risks, up 59 percent from the prior year. Given the increased concern and focus on cybercrime, incidents should show a decline or at least improvement in certain areas, but meanwhile a record 79 percent of respondents said they detected a security incident in the past 12 months – and that does not take into account the number of incidents that remain undetected. According to the survey data, one noticeable area for improvement is the amount of collaboration between security professionals in the industry. Only 25 percent of respondents said they were involved in in industry-specific Information Sharing and Analysis Centers (ISACs), virtually the same as the year before. However, many industry observers anticipate that President Obama's executive order should boost participation in information sharing initiatives.

"One of the key takeaways from this year's survey is the increased involvement from the government as a result of the continued climbing number of cyberattacks combined with organizations not moving to protect themselves fast enough," said Bob Bragdon, Vice President and Publisher, CSO. "With both government pressure/regulation and the increased oversight by companies' boards of directors, businesses have the opportunity to become much more collaborative in sharing information and raising the security protection standard even as cybercriminals continue to evolve and adapt quicker than organizations."

Outsiders Pose Increasing Threat to Organizations

The most frequently cited types of compromise are crimes committed by external threat actors, those who are not employees or third-party partners with trusted access to networks and data. Nearly one third (31 percent) of respondents said they had been hit by a phishing attack in 2014. Distributed denial of service (DDoS) attacks are becoming increasingly potent and are one of the most frequent types of cybersecurity incidents, cited by 18 percent of survey respondents. Ransomware, a comparatively new type of cybercrime, is also becoming more sophisticated and commonplace.

"Over the past year, the Secret Service saw an increase in cyber-related activity involving capable networks of transnational criminals targeting U.S. citizens and financial institutions," said Stuart Tryon, Special Agent in Charge of the Criminal Investigative Division, Secret Service. "Currently, subjects in Eastern Europe control many of the Internet web sites buying and selling illicitly obtained credit card data. The public and private sectors must continue to work collaboratively to share cybersecurity indicators and partner to conduct investigations in order to deter, disrupt and dismantle cybercrime networks."

Third-Party Risks Need More Attention from C-Suite

Due diligence of the security capabilities and practices of third-parties has emerged as a core requirement in the past year, in part because of prominent breaches beginning with attacks on business partners. This year, 62 percent said they evaluate the security risks of third-party partners and 57 percent said they do so for contractors, while only 42 percent of respondents consider supplier risks. Surprisingly, one in five (19 percent) of CEOs, COO and CFOs surveyed said they were not at all worried about any kind of supply chain risk. What's more, consider that only 16 percent of respondents said they evaluate third parties' cybersecurity more than once a year—and 23 percent do not evaluate third parties at all.

Boards are Concerned, but not Always Engaged

Another result of the barrage of breaches over the past year is that many boards of directors now take a very active interest in cybersecurity. They want to know about current and evolving risks, as well as the organization's security preparedness and response plans. The question is how often security leaders provide cyber risk briefings to their boards. Despite the increase in both incidents and associated damages, only 30 percent of respondents said their Chief Information Security Officer (CISO) or Chief Security Officer (CSO) makes quarterly security presentations to the board. One in four (26 percent) said their senior security executive presents once a year – and 28 percent said their security leaders make no presentations at all.

Cyberthreats: a Board Governance Issue

Cyberthreats are one of the most significant business risks facing organizations today. The National Association of Corporate Directors recommends oversight be a function of the full board. Yet, 30 percent of respondents said no board committee or members are engaged in cyber risks at all. At the other end of the spectrum, only 25 percent of respondents said their full board is involved in cyber risks. As boards of directors are held accountable, it is necessary to treat cybersecurity as an overarching corporate risk issue rather than simply an IT risk. Many have yet to adopt this approach, however. Almost half (49 percent) of boards view cybersecurity as an IT risk, while 42 percent see cybersecurity through the lens of corporate governance.

"If an organization's management—including boards of directors, senior executives, and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained," said Julia Allen, a principal researcher on the CERT cyber risk management team. "To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance."

The report outlines seven reasons why cybersecurity is a board governance issue:

1. The impact of cybersecurity is systemic. Incidents can impact an organization's global operations even when a risk point is thousands of miles away.
2. The financial impact can be huge, with losses measured in billions of dollars, including costly class-action lawsuits.
3. As regulations evolve, compliance is becoming more challenging and increasingly costly.
4. The Internet of Things has brought new threats that can cause extreme risks and tremendous physical damage.
5. Cybersecurity insurance should be considered as a regulatory hedge against cyber risks. A risk committee should ask questions regarding coverage for directors' and officers' liability, commercial general liability prior acts, and property and casualty insurance.
6. Adversaries such as nation-states and organized crime are working together to attack organizations for objectives like economic sabotage, theft of trade secrets, money laundering, terrorism, and military and intelligence operations.
7. Cyberattacks can result in substantial financial losses and damage brand reputation by disrupting an organization's strategic objectives, such as a planned merger or acquisition, the launch of a new product, or a business deal with a potential customer.

To download the full survey, visit: www.pwc.com/us/cybercrime.

Additional coverage on the 2015 U.S. State of Cybercrime Survey can be found at CSOonline.com.

Methodology
The 2015 US State of Cybercrime Survey was a collaborative effort among PwC, CSO, the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service. More than 500 executives of U.S. businesses, law enforcement services, and government agencies contributed. The survey evaluates trends in the frequency and impact of cybercrime incidents, cybersecurity threats, information security spending, and the risks of third-party business partners in private and public organizations. The survey also assesses how businesses are adapting to evolving expectations of the information security function and the board of directors.

Note to Editors: References to the 2015 State of Cybercrime Survey must reference PwC, CSO, the U.S. Secret Service and the Software Engineering Institute CERT Division at Carnegie Mellon University.

About CSO
CSO is the premier content and community resource for security decision-makers leading "business risk management" efforts within their organization. For more than a decade, CSO's award-winning website (CSOonline.com), executive conferences, strategic marketing services and research have equipped security decision-makers to mitigate both IT and corporate/physical risk for their organizations and provided opportunities for security vendors looking to reach this audience. To assist CSOs in educating their organizations' employees on corporate and personal security practices, CSO also produces the quarterly newsletter *Security Smart*. CSO is published by IDG Enterprise, a subsidiary of International Data Group (IDG), the world's leading media, events and research company. Company information is available at www.idgenterprise.com.

About the United States Secret Service
The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial and cybercrimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service, through their Electronic Crimes Task Forces, has established successful partnerships in law enforcement, business and academic communities – across the country and around the world – in order to effectively combat financial and cybercrimes. More information can be found at: www.secretservice.gov.

About the Software Engineering Institute and the CERT Division
The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. The SEI helps organizations make measurable improvements in their software engineering capabilities by providing technical leadership to advance the practice of software engineering. For more information, visit the SEI website at http://www.sei.cmu.edu. The CERT Division of the SEI is the world's leading trusted authority dedicated to improving the security and resilience of computer systems and networks and a national asset in the field of cybersecurity. For more information, visit http://www.cert.org.

About PwC US
PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms, which has firms in 157 countries with more than 195,000 people. We're committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com/US.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

# # #

Contacts:

For CSO:
Gregory Rosa
grosa@idgenterprise.com
508.766.5375

For PwC:
Jo Anne Barrameda McCusker
jo.anne.barrameda@us.pwc.com
917.689.7279

For Secret Service:
Robert Hoback
robert.hoback@usss.dhs.com

For CERT:
Richard Lynch
rlynch@sei.cmu.edu
412.268.408